车联网安全概述

1. 车联网安全用列概述
2. 车联网当前的标准规范简介
3. 车联网生态系统概述
4. 车联网系统通讯网络技术概述
5. 车联网子系统网络安全接口概述
6. 车联网和后续V2X及ITS概述及相应的安全因素
7. 国内车联网著名安全组织简介

1 车联网安全用列概述

1.车联网安全用列概述

1.1 远程接管并控制汽车。

1.2 随时熄火汽车。

1.3 监视汽车使用者。

1.4 解锁汽车，比如开车门，后备箱等。

1.5 偷窃汽车。

1.6 跟踪和记录汽车行驶轨迹并收集信息。

1.7 阻止汽车安全保护系统，比如失效安全气囊功能等。

1.8 安装各种恶意软件等。

2 车联网当前的规范和组织

2.1 基于3GPP的V2X相关标准http://www.3gpp.org

2.2 基于802.11P的相关标准http://standards.ieee.org/develop/wg/WG802.11.html

2.3 基于IEEE1609的相关标准 https://standards.ieee.org/develop/wg/1609.html

2.4 欧洲智能交通系统相关标准 https://www.etsi.org

2.5 美国智能交通系统相关标准 https://www.nhtsa.gov

2.6.中国交通运输部 http://www.mot.gov.cn

2.7 中国智能交通协会 http://www.itschina.org

2.8 中国智能网联汽车产业创新联盟 http://www.caicv.org.cn

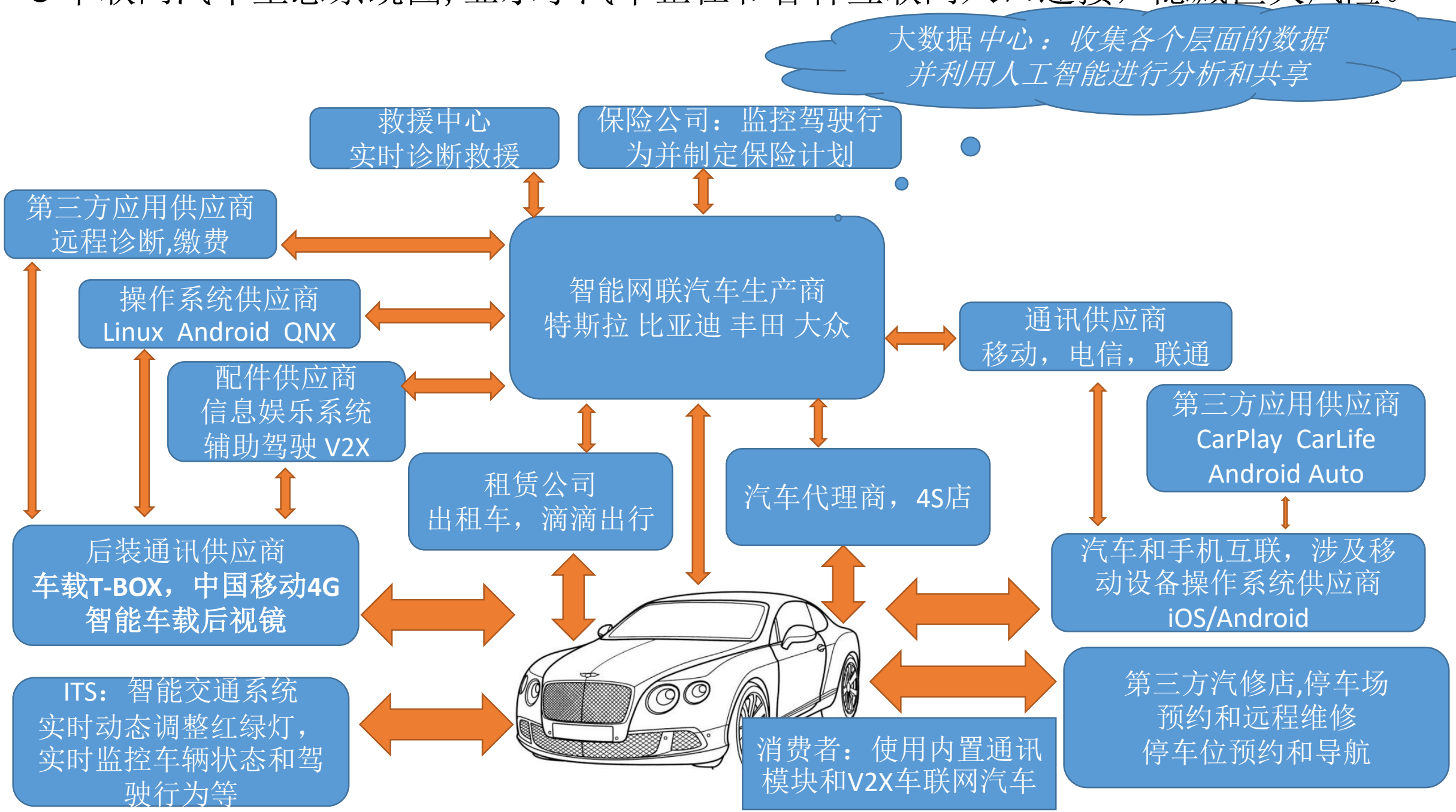
2.9 中国信息通信研究院 http://www.catr.cn

2.10 中国车载信息服务产业应用联盟 http://www.tiaa.org.cn

2.11 中国汽车工程协会 http://www.sae-china.org

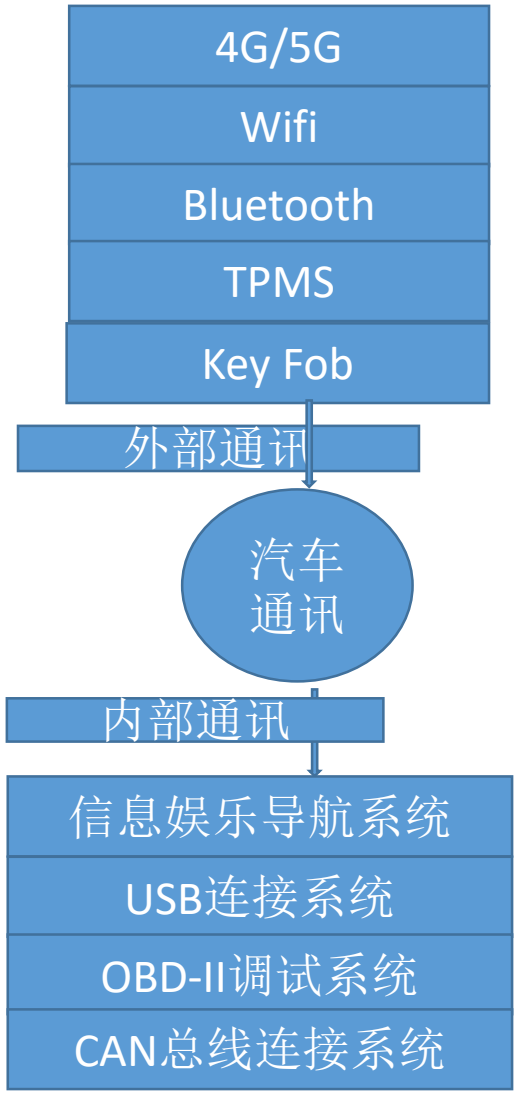
2.12 中国汽车工业协会 http://www.caam.org.cn

3 车联网汽车生态系统图, 显示了汽车正在和各种互联网入口连接，隐藏巨大风险。

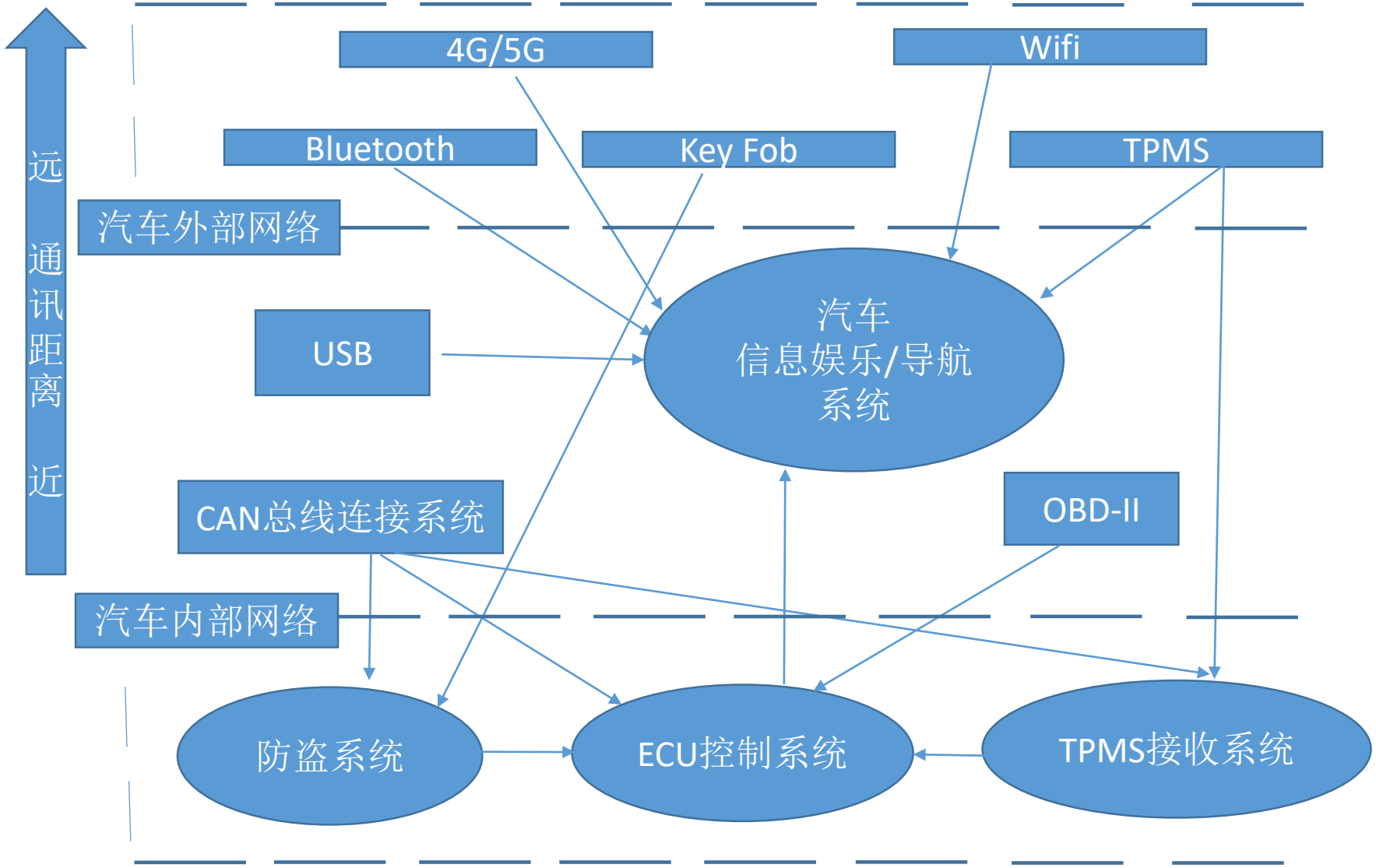


4 车联网系统网络通讯技术概述

汽车网络通讯概要图



汽车网络通讯网络详细图



5 车联网子系统网络安全概述

车联网安全可以归类为以下七个部分：

整体安全 硬件安全 操作系统基础安全 外部通讯安全 内部通讯安全 数据安全

车内和手机端应用程序安全 目前只关注下面三方面的安全。

5.1 汽车信息娱乐操作系统级安全

目前主流的汽车厂商广泛采用Freescale的基于ARM的iMX6/iMX8开发，目前部分高端车厂开始采用高通820A和英伟达的Tegra芯片，基本上是采用Linux,Android,QNX操作系统,而这部分涉及到基础系统安全，目前看存在长期不更新的问题，隐藏安全风险。

5.1.1 Linux + QT

5.1.2 QNX + QT

5.1.3 Android

5.1.4 USB接口风险（软件升级或恶意程序风险）

5.1.5 AUTOSAR(RTOS + MCU + CAN + Ethernet -> ECU)

5.1.6 百度的Apollo （Linux + ROS + Flask)

5 车联网子系统网络安全概述

5.2 汽车外部通讯网络系统安全接口

5.2.1 4G/5G

5.2.2 Wifi

5.2.3 Bluetooth

5.2.4 TPMS

5.2.5 Key fob

5.2.6 CAN

5.2.7 OBD-II

5.2.8 Automotive Ethernet

5 车联网子系统网络安全概述

5.3 汽车内部通讯网络系统接口

5.3.1 CAN （ISO-TP, CANopen）

ISO-11898 https://www.iso.org/standard/63648.html

https://github.com/linux-can/can-utils

https://github.com/CANopenNode/CANopenNode

5.3.2 Automotive Ethernet

802.3bw-2015 **https://ieeexplore.ieee.org/document/7433918/**

5.3.3 OBD-II

https://www.sae.org/standards/content/j2534/1_201510/

https://www.sae.org/standardsdev/groundvehicle/j1939a.htm

5.3.4 Lin, FlexRay, MOST

5.3.5 AUTOSAR

https://www.autosar.org

6 V2X车联网技术简述及网络安全因素

- V2X　Vehicle to Everything （车和所有事物通讯）
- V2V　Vehicle to Vehicle（车和车通讯）
- DSRC Dedicated Short Range Communication（专用短距离通讯）
- 目前V2X技术主要有两种实现方式，基于Wifi的DSRC和基于LTE/5G的V2X.
- DSRC V2V技术标准已经制定了10年，软件已经可以达到量产的标准，但需要重新部署大量的基站等设施，费用巨大，而且需要市面上的其他终端也支持这一技术，目前看不适合在中国大陆地区部署。
- LTE/5G V2X技术标准2018年已经完成制定，芯片已经面市，2019年开始商用部署5G，目前主要的推动者是高通（终端通讯设备主要供应商），华为和爱立信（两家通讯基础设施主要供应商），主要优势是可以复用升级现有的三大通讯运营商的基站设施。
- **安全风险** 全新的各种标准和协议必然导致有各种安全方面的问题,需要熟悉相应协议并进行安全渗透测试发现安全漏洞。

6 智能交通系统简述及网络安全因素

- ITS：Intelligent Transportation Systems（智能交通系统）
- 当前的交通系统只是进行红绿灯管控，交通违法抓拍，做不到实时，动态，智能等功能。
- 随着V2X车联网技术的到来，必定带来智能交通系统升级改造的机会。
- 根据实时车辆和行人的负荷进行动态调整红绿灯，是交通更通畅。
- 根据实时车辆故障通知其他车辆绕道，避免阻塞。
- 实时监控和跟踪车辆驾驶行为，减少违反和违法行为。
- 实时监控驾驶员行为，处理紧急故障和危险行为并进行远程控制。
- 结合大数据平台和深度机器学习技术，可以扩展在线业务办理比如自动年审等，以及监控和预防违法行为等。
- **安全风险**：基于各种通讯协议和交互应用的接口不断增加，必然带来大量潜在的安全问题。

7 车联网著名安全组织简介

7.1 中国汽车行业漏洞应急响平台 https://cavd.org.cn/index.html

7.2 中国汽车工业协会成立了智能网联汽车信息安全架构工作组，负责人：东软睿驰

7.3 中国车载信息服务产业应用联盟成立了车联网安全工作组，负责人：奇虎360公司

7.4 奇虎360公司的智能网联汽车安全实验室牵头成立了中国车联网安全联盟

7.5 奇虎360智能网联汽车安全实验室 http://skygo.360.cn

7.6 腾讯科恩实验室（2016/17年破解特斯拉并发现多个安全漏洞）

7.6 亚信智能汽车和自动驾驶安全团队